HP Atalla Network Security Processor

HP Atalla NSPは、DESおよびトリプルDESアルゴリズムに完全対応し、最新金融アプリケーション、ICカード・アプリケーションにおけるHSM（Hardware Security Module）のスタンダードとしてご利用いただけます。

HP Atalla Ax150シリーズNSP（ネットワーク・セキュリティ・プロセッサ）は、さまざまなタイプのトランザクションを保護するトリプルDESおよびその他先進の暗号キーのために比類のない論理的セキュリティを提供するAtalla Security Productsの最新シリーズです。HP Atalla Ax100シリーズと完全な互換性を保ち、Atalla独自の鍵管理ソリューションAtalla Key Blockを使用して業界屈指の先進の鍵管理を実現します。新しいHP Atalla Ax150シリーズNSPは、米国連邦政府情報処理規格（FIPS）140-2の最強レベル4の認定を受けており、物理面および管理面において最高レベルのセキュリティ要件を満たしています。さらに、RoHS指令に準拠し環境面への配慮も強化しました。

A10150 NSP

HPが提供する最新の高性能NSPです。トリプルDESおよびそのほかの暗号キーを比類ないレベルで保護し、大容量トランザクション環境に対応します。

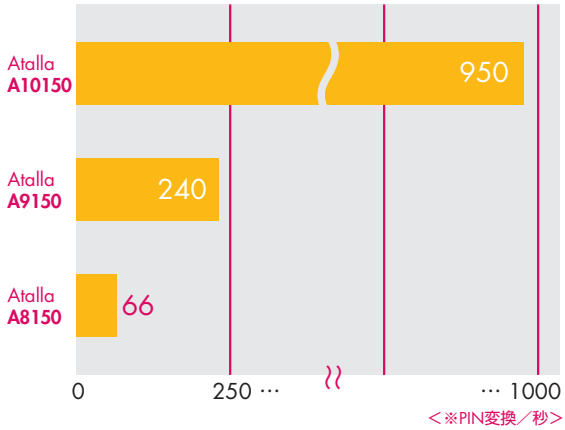
A9150 NSP

ミッドレンジのトランザクション環境用に最適化された最新のNSPです。トリプルDESおよびそのほかの暗号キーを比類ないレベルで保護し、重要なトランザクションの安全性を保護します。

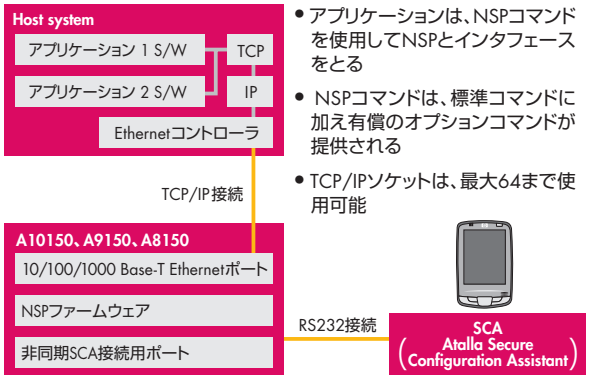
A8150 NSP

エントリレベルの処理環境に対応し、トリプルDESおよびそのほかの暗号キーを比類ないレベルで保護します。

■トリプルDES性能表



■Atalla NSPシステム構成



- アプリケーションは、NSPコマンドを使用してNSPとインタフェースをとる
- NSPコマンドは、標準コマンドに加え有償のオプションコマンドが提供される
- TCP/IPソケットは、最大64まで使用可能

※一秒あたりに実行可能なPIN（Personal Identification Number）のトリプルDES暗号化（または複合化）処理

HP Atalla Network Security Processor

もはやネットワークなしにはビジネスが成り立たない現在、ネットワークの頑強なセキュリティは企業の責務となっています。HP Atalla NSPは、30年以上の実績を持ち、また操作の容易性から、金融ネットワークのセキュリティを必要とする主要金融機関、ISV、世界中のパートナーから採用されてきました。さらに、Atalla Key Blockを使用することで、業界でもっとも安全なトリプルDESおよびそのほかの先進の暗号メカニズムを実装し、機密データのための妥協ないセキュリティ、高性能処理、高速ホスト接続を実現します。

HP Atalla Ax150シリーズのラインアップ

Atalla Ax150シリーズNSPは、大規模なエンタープライズ環境から小規模環境まで、必要となる処理性能に合わせ3種類のモデルを提供します。

- A10150 NSP—ベンチマークで1秒あたり950のトリプルDES PIN変換を達成した、大容量トランザクション環境向けの最新NSP
- A9150 NSP—ミッドレンジのトランザクション環境向けNSP。1秒あたり240のトリプルDES PIN変換を達成し、コスト効果の高いソリューションを提供
- A8150 NSP—1秒あたり66のトリプルDES PIN変換の性能で、小規模環境に最高レベルの暗号キー保護を実現

物理的セキュリティ

Atalla NSPは、ハード面において以下のような堅牢な設計を採用しています。

- FIPS 140-2レベル4に準拠
- ラックマウント（2U）型の堅牢なフォームファクタ
- Medicoロックつきのダブル・ロック式ベゼル
- 外部からの侵入に対する保護（保護グリッド）
- 範囲外の温度と電圧の検知
- バッテリ電圧の低下から保護
- MFK（Master File Key）をハードウェア内に保存し、外部からの不正な攻撃を遮断

AKBが実現する論理的セキュリティ

NSPの堅牢性とAtalla Key Blockの論理的な鍵管理アーキテクチャの組み合わせによって、高度なセキュリティ機能を実現します。

- ANSI X9.24 1-2004に準拠
- 高度なセキュリティ・アーキテクチャにより、PIN、キー、その他機密データのクリアテキスト形式での取得を防止
- 自動および手動の鍵管理オプション
- Atalla Secure Configuration Assistant（SCA）による、暗号化されたキーロード（キーまたはキー・コンポーネントをクリアテキストで渡さない）
- ATM公開キーのサポートによるリモートからのATMキーロード
- 改ざんを防止するアーキテクチャ

高速ホスト接続

TCP/IPを使用し、ホストとの高速接続を容易に実現します。

- TCP/IP用の自動認識の10/100/1000Base-T Ethernetインタフェース
- 高性能のTCP/IPスタックと通信プロセッサを統合

柔軟性と拡張性

ユーザ環境やアプリケーションに幅広く対応し、多様なユーザ要件を満たします。

- さまざまなアプリケーションをサポート（ATM、EFT、POS、ストアドバリュー、ロイヤリティ・カード、企業間資金移動など）
- ユーザ定義のセキュリティ・ポリシーの実装
- 容易なコマンドセットとカスタマイズ
- Atalla以外の環境とのシームレスな相互運用
- Atalla公開キーのサポート
- Atalla NSPの初期モデルとのコマンドセットの互換性維持

運用性

セキュリティを確保しながらも、運用性を考慮した設計であり、主要金融機関等より高い支持を受けています。

- SCAによる容易なキーロード
- GUIによるAtalla Key Blockのキーロード
- CD-ROMを使用した迅速で簡単なリリース・アップグレード
- アップグレード時にEPROMなどのファームウェア・コンポーネントの交換が不要

Atalla Key Blockとは

Atalla Key Block(AKB)とは、Atalla独自の論理的な鍵管理アーキテクチャです。これにより、旧来の脆弱な鍵管理によって生じる攻撃されやすいトリプルDESセキュリティの問題を解決します。業界標準をリードし、シンメトリックな鍵管理方式を規定するANSI X9.24 Part1-2004に準拠する唯一の製品です。改ざん防止の機能を持ち、暗号保護のスタンダードを向上させています。

AKBのアーキテクチャ

AKBはヘッダ、キー・フィールド、MACの3つの構成要素を持ち、暗号化キーを論理的に管理・保護します。

ヘッダ

- クリアテキストで構成され、キーの利用を制御

キー・フィールド

- Master File Keyによってキー値を保護
- 可変長キー(8、16、24またはそれ以上)のサポート
- キー長(8、16、24)に関わらず、すべて48バイトになるようにパディングし、短い脆弱なキーの存在を隠蔽
- トリプルDESにより暗号化

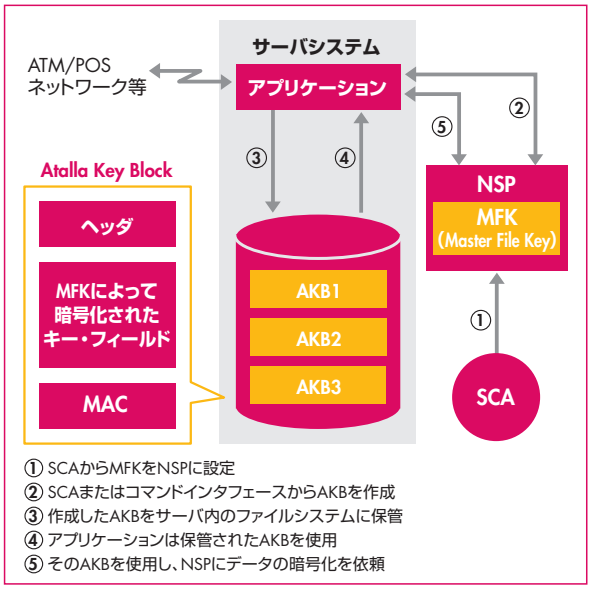
メッセージ認証コード(MAC)

- キー・フィールドとヘッダをトリプルDES暗号化しMACを算出
- MAC値の比較によりキー・フィールドの完全性を保持

容易な操作性

- キーをAKB化することでサーバ内での安全な鍵の保管を実現
- セキュリティに関する予備知識のないユーザでも簡単に理解および管理可能
- 属性はASCII文字または数字で表現
- 旧バージョンからの包括的な移行のガイドラインの提示とサポート
- キー変換コマンドにより、Atallaの異なる構造から新しいAtalla Key Blockに変換可能
- SCAのGUIにより、正確かつ容易にキーロードを実行

Atalla Key Block(AKB)による論理的な鍵管理



HP A×150シリーズが対応するスタンダード一覧

暗号方式サポート	・データ暗号化アルゴリズム(DEA)(ANSI X3.92-1987、ISO 10126-2)、DES、2倍長および3倍長キーのトリプルDES ・メッセージ暗号化の銀行手続き、一般原則 (ISO 10126-2) ・PIN 管理とセキュリティ、パート1および2 (ANSI X9.8、ISO 9564-1および2) ・メッセージ認証 (ANSI X9.9-1987、ISO 9807) ・マスターカードCVC(カード検証コード)、Visa CVV(カード検証値)、アメリカン・エキスプレスCSC(カード・セキュリティ・コード) ・トランザクションごとの固有キー (ANSI X9.24-1990) ・EMVベースのスマートカードのサポート
PIN認証方式	・Atalla Identikey ・IBM 3624 ・Visa PVV (PIN Verification Value) ・Atalla Bi-Level DES ・Diebold ・NCR
PINブロック形式	・米国規格協会(ANSI X9.8-1982) ・PIN Pad ・IBM 324 ATM PIN Format ・Unisys (Burroughs) ・Diebold ・Docutel/Olivetti ・Visa Derived Unique Key Per Transaction
鍵管理規格	・ANSI X9.17-1985 ・ANSI X9.24-2004 ・ANSI X9.52

A10150 NSP / A9150 NSP / A8150 NSP

寸法	高さ	8.71cm（3.43インチ）
	幅	48.49cm（19.25インチ）
	奥行	74.29cm（29.25インチ）
	重量	23.75kg（57.35ポンド）
制御		電源オン／オフ用スイッチ
電気的仕様	入力電圧 （デュアル入力、自動認識）	AC100から120V（3A、50/60Hz）、AC200から240V（1.5A、50/60Hz）
	消費電力	AC120Vで平均1.8A、電源オン時に最大3.25A
動作環境	温度（推奨値）	+20°C～+25°C
	湿度（推奨値）	40%～50%（結露しないこと）
認証／準拠	安全性	UL/CSA/TUV
接続方法	通信方法	TCP/IP使用のEthernet
	インタフェース	10/100/1000Base-T（RJ45、自動認識）

⚠ 安全に関するご注意　ご使用の際は、商品に添付の取扱説明書をよくお読みの上、正しくお使いください。水、湿気、油煙等の多い場所に設置しないでください。火災、故障、感電などの原因となることがあります。

お問い合わせはカスタマー・インフォメーションセンターへ
03-6416-6512　月～金 9:00～19:00　土 10:00～18:00（日、祝祭日、年末年始および5/1を除く）
HP Atalla 製品に関する情報は
http://www.hp.com/jp/atalla

本カタログは環境保護のため100%再生紙および大豆インキを使用しています。

記載されている会社名および商品名は、各社の商標または登録商標です。
記載事項は2006年12月現在のものです。
本カタログに記載された内容は、予告なく変更されることがあります。
© Copyright 2006 Hewlett-Packard Development Company,L.P.

日本ヒューレット・パッカード株式会社
〒102-0076 東京都千代田区五番町7番地

JTN06215-01